

## UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

7744 Chesterbrooke Drive, Greensboro, North Carolina,  
27455-3055

Case No. 1:20mj 242

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the \_\_\_\_\_ Middle \_\_\_\_\_ District of \_\_\_\_\_ North Carolina \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1343

18 U.S.C. § 1956

Wire Fraud

Money Laundering

Offense Description

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

15/Charles Parker LPA

Applicant's signature

Charles Parker, Special Agent, HSI

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date:

08/14/20

L. Patrick Auld

Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld, United States Magistrate Judge

Printed name and title

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to items and information associated with the SUBJECT PREMISES:  
7744 Chesterbrooke Drive, Greensboro, North Carolina, 27455-3055.

The SUBJECT PREMISES can be further described as:

A two story light colored brick single family home with a gray shingled roof and a mahogany double front door that is arched at the top and surrounded by ivy. The house is set on an approximately 2.21 acre lot with a circle driveway leading from the street to the front of the house.

A photograph of the SUBJECT PREMISES is below:



## **ATTACHMENT B**

### **Items at Premises to be Seized by the Government**

The items to be seized are any evidence, fruits, and instrumentalities of a scheme to defraud investors in Airbit Club and to launder the proceeds of that scheme to defraud (the "Airbit Club Scheme") in violation of Title 18, United States Code, Sections 1349 (conspiracy to commit wire fraud), 1349 (conspiracy to commit bank fraud), and 1956 (conspiracy to commit money laundering) (collectively, the "Subject Offenses"), in the form of the following:

1. Documents, photographs, and information, in whatever form, showing possession, occupancy, dominion, and control over the SUBJECT PREMISES.

2. Records, documents, and items that constitute evidence of concealment of the Subject Offenses, in the form of: financial records, ledgers, or other items demonstrating attempts to keep financial transactions out of a bank or off a regulated cryptocurrency exchange; documents or records demonstrating steps taken to conceal the source or ownership of funds; records or items demonstrating attempts to conceal participation in the Airbit Club Scheme or to create or provide documents showing an alternate source of income or employment; evidence of use of burner cellphones or encrypted messaging application to conceal communications with other participants or members of the Airbit Club Scheme.

3. Documents, photographs, and information, in whatever form, containing personally identifiable information, banking information, cash transactions, or cryptocurrency information of people believed to be victims of the Airbit Club Scheme.

4. Business and financial records, in whatever form, of Airbit Club and Galaxy Success, Inc., and related entities, or related to CECILIA MILLAN or other participants or members of the Airbit Club Scheme including but not limited to, bank account and credit card



statements, checks, deposit slips, deposit items, cashier's checks, money orders, wire transfers, cash withdrawals, cryptocurrency wallets, and recovery seeds.

5. Documents, photographs, and information, in whatever form, showing promotion or advertisement of the Airbit Club Scheme or attempts to recruit additional individuals to invest in the Airbit Club Scheme.

6. Evidence concerning the proceeds of the Airbit Club Scheme in the form of United States and/or foreign currency, coins or bars of precious metals, jewelry, documentation of financial transactions, bank statements, checks, books, records, invoices, payment receipts, money orders, cashier's checks, bank checks, safe deposit box keys, money wrappers, filed and non-filed income tax records, credit card receipts, credit card statements, minute books and other items evidencing the obtaining, secreting, transferring, and/or concealment of assets and the obtaining, secreting, transferring, concealment, and/or expenditure of money as part of the Airbit Club Scheme.

7. Any laptop computers, desk top computers, electronic tablets, smart mobile telephones, and any other devices capable of storing data and accessing websites for the purpose of committing the Subject Offenses ("COMPUTERS").

### **COMPUTERS**

The term "computer," as used here, is defined as an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

1. Any computers (including file servers, desktop computers, laptop computers, mainframe computers, smart phones, and mobile devices), input/output devices,

software, documentation, data security devices and storage devices (such as hard drives, Zip disks, floppy disks and thumb drives) that are found on the premises to be searched, in order to examine those items for records as described in this list of Items To Be Seized. Smart phones, cellphones or other mobile devices will be limited to those associated with Relevant Parties.

2. Any records, documents, materials and files described elsewhere in this attachment which are maintained on a computer or preserved in files that have been "deleted" from computer storage devices or facilities. The terms "records", "documents", "materials", and "files" include all information preserved in any form, visual, magnetic, electronic or aural, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise. These definitions apply regardless of the form in which such records, documents, materials and files, including any drafts or modifications, may have been created or stored; any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as writing, printing or typing); any computerized, electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device, such as hard disks, CD-ROMS, optical discs, printer buffers, smart cards, memory calculators, electronic dealers, Thumb Drives, Flash media, ZIP drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).
3. Special agents are authorized to seize and remove from the premises any computer hardware including computer system input/output (I/O) peripheral devices and

software so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

4. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.
5. Special agents and computer analysts working with special agents are authorized to seize the relevant system software (operating systems, interfaces, and hardware drivers), any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices, including, but not limited to, passwords, keycards, and dongles. In addition, they are authorized to reconfigure the system as it now operates in order to accurately retrieve the evidence stored therein.
6. In regard to the inspection of computers and the context of related equipment for records, documents, materials and files within the scope of this warrant, special agents are authorized to analyze the electronically stored data, whether on-site or in a laboratory or other controlled environment, using the following techniques: (a) surveying various file "directories" and the individual files they contain in order to locate evidence and instrumentalities authorized for seizure by the warrant; (b) "opening" or reading the first few "pages" of such files in order to determine their

precise contents; (c) "scanning" storage areas to discover and possibly recover deleted data; (d) "scanning" storage areas for deliberately hidden files; and (e) performing electronic "key word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

7. This warrant specifically authorizes the creation of a "mirror image" of a drive or other storage device or media for use in an off-site search. In that event, the agents are authorized to use the above search techniques, for said search.

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF:

**7744 CHESTERBROOKE DRIVE,  
GREENSBORO, NORTH CAROLINA 27455-3055**

Case No. 1:20-mj-242

~~Filed Under Seal~~

*WPA*

**AFFIDAVIT IN SUPPORT OF  
APPLICATION FOR SEARCH AND SEIZURE WARRANTS**

I, CHARLES PARKER, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent (SA) of the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and have been so employed since 2019. I am currently assigned to the HSI Winston-Salem Office, where my duties include, among others, investigating violations of Titles 8, 18, 19, 21, and 31 of the United States Code (U.S.C.). Prior to reporting for assignment, I attended training at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia, where I received instruction in Federal criminal statutes, search, seizure and arrest authority, and many other facets of federal law enforcement. Before joining HSI, I was a Special Agent of the United States Secret Service (USSS) where I was assigned to the USSS Boston Office for four years. My duties included investigating financial crimes and computer-based attacks on the nation's financial, banking, and telecommunication infrastructures. Prior to the USSS, I was a police officer in Greensboro, North Carolina for 10 years. During that time, I drafted over 50 search warrants and participated in over



500 felony investigations. These investigations resulted in arrests, seizures, interviews, and prosecutions in local, state, and federal courts.

**STATUTES VIOLATED, PREMISES TO BE SEARCHED, AND  
PROPERTY TO BE SEIZED**

2. Based on the facts as set forth in this affidavit, I submit there is probable cause to believe that CECILIA MILLAN ("MILLAN") has committed violations of Title 18, United States Code, Sections 1349 (Wire Fraud Conspiracy), 1349 (Bank Fraud Conspiracy) and 1956(h) (Money Laundering Conspiracy) (collectively, the "Subject Offenses").

3. This affidavit is made in support of an application for a warrant to search the location specifically described in Attachment A, the premises located at 7744 Chesterbrooke Drive, Greensboro, North Carolina, 27455-3055 (the "SUBJECT PREMISES"). This request also includes any computers, cell phones, and other electronic devices found at the SUBJECT PREMISES during the execution of the search warrant, which are owned or controlled by MILLAN. As set forth herein, there is probable cause to believe that evidence of the Subject Offenses, which is more specifically described in Attachment B of this Affidavit, will be found on the SUBJECT PREMISES. The facts and information in this affidavit are based upon my personal knowledge as well as the observations of other law enforcement agents and others involved in the investigation.

4. The facts and information in this affidavit are based upon my personal knowledge as well as the observations of other law enforcement agents and others involved in the investigation.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

**JURISDICTION**

6. This Court has jurisdiction to issue the requested search and seizure warrants to obtain evidence of a crime; contraband, fruits of a crime, or other items illegally possessed; or property designed for use, or used in committing a crime as defined by Rule 41(c)(1)-(3).

### **PROBABLE CAUSE**

7. On or about August 13, 2020, MILLAN was indicted by a grand jury sitting in the Southern District of New York with violations of Title 18, United States Code, Sections 1349 (Wire Fraud Conspiracy) and 1956(h) (Money Laundering Conspiracy).<sup>1</sup> There is also probable cause to search the information described in Attachment A for evidence of the Subject Offenses as further described in Attachment B.

### **Probable Cause Summary**

8. Since in or about February 2019, HSI has been investigating a large-scale international Ponzi scheme involving “Airbit Club,” a purported cryptocurrency<sup>2</sup> investment and

---

<sup>1</sup> The August 13, 2020 indictment charging MILLAN also charged PABLO RENATO RODRIGUEZ, GUTEMBERG DOS SANTOS, and SCOTT HUGHES with violations of Title 18, United States Code, Sections 1349 (Wire Fraud Conspiracy), 1349 (Bank Fraud Conspiracy) and 1956(h) (Money Laundering Conspiracy) and charged JACKIE AGUILAR with violations of Title 18, United States Code, Sections 1349 (Wire Fraud Conspiracy). MILLAN has not been charged with the bank fraud conspiracy at this time.

<sup>2</sup> Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and then generate, store, or generate and store public and private keys used to send and receive cryptocurrency. A public key, or public address, is akin to a bank account number, and a private key, or private address, is akin to a PIN number or password that allows a user to access and transfer value associated with the public address or key.

mining company that promises to earn its investors profits in exchange for cash investments in the form of club “memberships,” which each cost \$1,000 (the “Scheme”). As set forth in greater detail below, the Scheme was created by PABLO RENATO RODRIGUEZ and GUTEMBERG DOS SANTOS in late 2015, and has operated through several mid-level managers of the Scheme, including MILLAN, and others. MILLAN’s role in the Scheme is to promote Airbit Club to investors and to launder the proceeds of the Scheme. While RODRIGUEZ, DOS SANTOS, MILLAN, and other Master Council members—the most senior promoters of the Airbit Club Scheme—are primarily responsible for perpetrating the Scheme, SCOTT HUGHES, an attorney and purported attorney for Airbit Club, is instrumental in laundering the proceeds of the Scheme and transferring those proceeds to RODRIGUEZ, DOS SANTOS, MILLAN, and other members of the Master Council.

9. During its investigation, HSI has interviewed several individuals (the “Victims”) who each invested thousands of dollars in the Scheme. As set forth in greater detail below, beginning in approximately 2015, certain Victims were told that their money was being invested in, among other things, Bitcoin mining technology, and that Victims would earn money as a result of Airbit Club’s use of specialized cryptocurrency technology. Other Victims were simply told that, in exchange for keeping \$1,000 invested in an Airbit Club “membership,” each Victim would receive approximately \$4 to \$13 per day in guaranteed returns on that “membership.” Victims were able to login to an online Airbit Club portal and view the purported returns on their investments (the “Online Portal”). Initially, Victims were able to withdraw funds from their Online Portal either in Bitcoin or in cash. By 2018, Victims became unable to withdraw funds from their account, were charged significant fees in order to withdraw funds, or were forced to convert their account balance into an Airbit Club-created cryptocurrency called “Traxalt” in order

to withdraw funds. When Victims filed complaints with law enforcement, their access to the Online Portal was terminated, and their so-called “accounts” disappeared. Based upon my participation in this investigation, Airbit Club does not appear to be engaged in any legitimate Bitcoin mining operations and instead appears to operate as a Ponzi scheme, where so-called “returns” to investors are in fact the funds invested by other individuals later in time.

**Victim-1, AGUILAR and the Texas Scheme**

10. On or about May 29, 2019, HSI interviewed a Victim based in the Dallas, Texas, area (“Victim-1”) who told HSI, in substance and in part, the following:

a. In or about January 2018, Victim-1 attended a presentation about Airbit Club at Victim-1’s local library. At the presentation, representatives of Airbit Club, including JACKIE AGUILAR and a second coconspirator (“CC-1”), offered Victim-1 and others an opportunity to invest in an Airbit Club “membership.” For each \$1,000 membership, Victim-1 was promised daily returns between \$7 and \$13.

b. Victim-1 initially purchased eight memberships for a total investment of \$8,000. Victim-1 was instructed by AGUILAR to purchase the memberships in cash, to which Victim-1 agreed and provided \$8,000 in cash to AGUILAR.

c. After Victim-1’s purchase, Victim-1 was provided login information for the Online Portal, where Victim-1 could view his/her account balance and see the daily returns accrue in his/her account.

d. Victim-1 was told by AGUILAR that Victim-1 would earn more money by recruiting additional investors in Airbit Club.

e. Beginning in approximately July 2018, the Online Portal was shut down for several weeks and Victim-1 was unable to login to make withdrawals or view Victim-1’s account

balance. Victim-1 asked AGUILAR and CC-1 about the Online Portal and why it was it shut down. In response, AGUILAR hosted a meeting both in person and via an online broadcast in which AGUILAR insisted the Online Portal was being “upgraded” and promised it would be functional soon.

f. In addition, around the middle of 2018, Airbit Club began charging Victims fees in order to make withdrawals from their accounts (the “Fee Increase”). While Victims were previously charged an approximate 4% fee to withdraw funds from their accounts, in the middle of 2018, the fees were increased to approximately 40%. None of these fees were disclosed to Airbit Club Victims prior to their purchase of memberships. Airbit Club also began charging Victims a \$35 per transaction fee for withdrawals and capping individual withdrawals at \$500 each. As of approximately May 2019, Victim-1 had requested approximately \$8,000 in withdrawals from the Online Portal, but had received only approximately \$4,000 due to the Fee Increase. Victim-1 asked both CC-1 and AGUILAR about these fees.

g. Later in 2018, Airbit Club began requiring Victims to convert the funds in their account into a purported cryptocurrency called Traxalt in order to make withdrawals. Victims were again charged fees for conversion to Traxalt, and were told that the value of Traxalt could decrease without warning.

h. On or about June 18, 2019, MILLAN and AGUILAR hosted a conference call for “Elite Team” investors in the Airbit Club Scheme, that is, investors below MILLAN. HSI monitored and recorded the call with the consent of Victim-1, who was participating in the call. During the call, MILLAN and AGUILAR made a number of statements, including in sum and substance:



i. MILLAN and AGUILAR acknowledged that Victims were struggling to withdraw their money from Airbit Club. MILLAN and AGUILAR claimed that the delayed payouts were caused by a cap of 250,000 bitcoin transactions per day that can be recorded on the bitcoin blockchain and by the rising and fluctuating cost of bitcoin, among other excuses. AGUILAR and MILLAN told the Victims that using Airbit Club's own cryptocurrency, Traxalt, would enable them to withdraw their money quickly and to "retire."

j. MILLAN and AGUILAR also discouraged complaining Victims from requesting payouts from Airbit Club, despite prior demands for withdrawals. MILLAN stated, "I'm gonna tell you something. I've earned like ten million dollars in AirBit Club in the past three and a half years. . . But I want to tell you that I don't do payouts. You want to know why I don't do payouts? Because I maximize. My business is in building. I want you to know that the people who never do payouts are the ones who earn more. They earn more, why? Because instead of taking 100 percent of their commission and they . . . because of . . . the margin of protection, the price of bitcoin, because the cost of 8 percent of AirBit, instead of losing 35 to 40 percent, we won!" MILLAN (with AGUILAR on the line) also stated that AGUILAR had earned "over seven figures" so far by investing with Airbit Club.

k. AGUILAR ended the call by telling Victims, "I'm just saying . . . investors are investors that you put their money and let it grow, and hold onto and let your bitcoin grow in your wallet as well, with the fluctuation where bitcoin is growing more. Or you grow the business and maximize it, where we're able to cash one another out. . . . So when somebody comes in, it's a thousand dollar membership for bitcoin, because remember, 70-30, 30 goes to the Backoffice so they can open it. And 70 we can cash out people as they're coming in. So that money goes in your blockchain wallet and grows and fluctuates. So the opportunity is huge. It's

like how many bitcoin do ya'll wanna make? How much money do ya'll wanna make?" With this statement, AGUILAR acknowledged that their purportedly guaranteed returns in fact depended on the continued recruitment of new investors.

1. Victim-1 requested funds from Victim-1's Airbit Club account in July 2019, but has not received those funds.

### **Victim-2 and the Illinois Scheme**

11. In addition, on or about June 7, 2019, HSI interviewed a Victim based in the Chicago, Illinois, area ("Victim-2") who told HSI, in substance and in part, the following:

a. In or about mid-2018, Victim-2 attended a presentation for Airbit Club at a private residence attended by approximately twenty people and hosted by a participant in the Airbit Club Scheme ("CC-2"). During the presentation, CC-2 told Victim-2 that if Victim-2 invested in Airbit Club memberships, Victim-2 would double his/her investment in one year. CC-2 told Victim-2 that Victim-2 could earn additional returns by recruiting additional investors in Airbit Club.

b. Victim-2 understood that MILLAN worked for PABLO RENATO RODRIGUEZ, whom Victim-2 understood to be the founder and head of Airbit Club.

c. Approximately one week after the presentation hosted by Individual-2, Victim-2 invested \$16,000 in Airbit Club, which Victim-2 understood to represent 16 memberships in Airbit Club. Victim-2 earned \$4,000 profit, which was reflected in the Online Portal, and used that \$4,000 in profit along with \$12,000 cash to purchase an additional 16 memberships, for a total of \$32,000 in Airbit Club memberships.

d. Throughout 2018, Victim-2 was able to make only small withdrawals from Victim-2's Airbit Club account, but was charged fees of 40-50% per withdrawal, as well as per

transaction fees. Victim-2 was not informed of these fees at the time of Victim-2's investment. Over time, Victim-2 was only able to withdraw approximately \$4,000 from Victim-2's Airbit Account, even though Victim-2's account purported to show that Victim-2 had over \$32,000 available for withdrawal. Victim-2 contacted MILLAN and CC-2 regarding Victim-2's inability to make withdrawals, but neither MILLAN nor CC-2 would allow Victim-2 to make additional withdrawals, and both refused Victim-2's requests to have MILLAN or Airbit Club purchase Victim-2's memberships.

e. In or about January 2019, Victim-2 filed a complaint with the Illinois Attorney General's Office related to Airbit Club (the "Victim-2 Complaint"). When Victim-2 told CC-2 about the Victim-2 Complaint, Victim-2 received a WhatsApp message from MILLAN indicating that MILLAN was reporting Victim-2 to Airbit Club customer support. Approximately one week later, Victim-2 received a notice that her Airbit Club account was suspended, and Victim-2 was removed from the Airbit Club Facebook and WhatsApp groups. Victim-2 has not recovered the money invested in Airbit Club.

#### **Airbit Club Promotion and Responses to Victim Complaints**

12. Based on publicly available information about Airbit Club and information obtained pursuant to search warrants for Facebook, email accounts, and cellphones, including photographs and videos, I have learned, in substance and in part, the following:

a. Airbit Club's promotional activity includes several large-scale, lavish "galas" at which RODRIGUEZ, DOS SANTOS, and members of the Master Council, including MILLAN, dress in flashy clothes, talk about their professional successes, and throw parties that, they claim, are some of the fruits of their investment in Airbit Club. These promotional events

occur all over the world, and are large-scale “expos” in Latin America, the Middle East, Asia, and Russia.

b. RODRIGUEZ, DOS SANTOS, MILLAN, CC-3, and other members of the Master Council also promote Airbit Club on social media, such as Facebook, Instagram, and YouTube, including by posting promotional videos about Airbit Club.

c. RODRIGUEZ, DOS SANTOS, and MILLAN received complaints from Victims regarding Airbit Club as early as 2016. For example,

i. In or about July 2016, a Victim sent multiple complaints by email to a former Master Council Member, in sum and substance, that the Victim had not received his requested payout of his investments in Airbit Club and that Airbit investors were receiving payment for Bitcoin at prices far lower than the price of Bitcoin in the market. The former Master Council Member forwarded those emails from the Victim to RODRIGUEZ.

ii. In or about August 2016, a Victim emailed MILLAN advising MILLAN, in substance and in part, that the Victim intended to report Airbit Club to the “FBI” because the Victim had concluded that Airbit Club was “an illegal Ponzi scheme” on the basis that the Victim’s initial request for a payout was granted, but Airbit Club did not honor later, larger payout requests and that instead RODRIGUEZ provided the Victim with excuses for the delayed payout. MILLAN forwarded the Victim’s email to “bidsclub@gmail.com,” (the “Bidsclub Email”) an account controlled by DOS SANTOS.<sup>3</sup>

---

<sup>3</sup> Email addresses used by MILLAN or RODRIGUEZ commonly contain some or all of their name or initials, as do many other accounts used by DOS SANTOS. We believe the Bidsclub email, which is the email account associated with the “MasterPro1” account on the Online Portal, is controlled by DOS SANTOS because (1) the recovery phone number is DOS SANTOS’s cellphone number, (2) many emails in the account, including emails from Cloudflare, the entity

### **Laundering the Airbit Club Scheme Proceeds**

13. Based on my review of bank records for accounts controlled by RODRIGUEZ, DOS SANTOS, MILLAN, and HUGHES, information obtained pursuant to search warrants for email accounts and cellphones, and interviews with Victims, I have learned that Victims were directed by Airbit Club promoters, including CC-2, to provide their investments in cash, and many complied with that direction. Early in the Scheme, Master Council members collected cash from Victims and provided that cash to RODRIGUEZ either by depositing it into their own personal bank accounts and transferring the funds to RODRIGUEZ or by doing cash drops directly. MILLAN appears to have used her personal and business accounts to transfer Victim cash to RODRIGUEZ. From late 2015 through early 2016, MILLAN deposited more than \$350,000 in cash into a business account she controlled in the name of Galaxy Success, Inc. Between April and July 2016, that account transferred approximately \$136,000 to a RODRIGUEZ-controlled account in the name of Master Holdings Inc.

14. Based on my involvement in the investigation, my review of bank records and cryptocurrency transactions, and witness interviews, I have learned, in substance and in part, that:

a. Beginning in 2018, MILLAN moved away from transferring cash directly to RODRIGUEZ and began using the services of a third-party Bitcoin broker based in Panama ("CW-1").<sup>4</sup> According to CW-1, CW-1 met a Panama-based Airbit Club promoter ("CC-4"),

---

hosting the Online Portal, are addressed to "Gutenberg" and indicate a credit card in his name is used to pay the bill for Cloudflare, (3) many IP logins for the Bidsclub Email are in Brazil (DOS SANTOS's native country), and (4) many of the communications in the account are in Portuguese (DOS SANTOS's native language).

<sup>4</sup> In mid-2019, CW-1 was arrested in Panama and charged by the Eastern District of Louisiana with conspiracy to import narcotics. CW-1 is cooperating with law enforcement in hopes of



who worked under MILLAN. CC-4 introduced CW-1 to MILLAN, and MILLAN asked CW-1 about purchasing Bitcoin. To facilitate the transactions with MILLAN, CW-1 asked her to send fiat currency to a bank account CW-1 provided in exchange for CW-1 sending Bitcoin to a Bitcoin wallet identified by MILLAN. CW-1 charged 6% and CW-1's account holder charged 2% per transaction. CW-1 estimated that CW-1 sold MILLAN Bitcoin this way multiple times prior to July 2018.

b. In July 2018, MILLAN attempted to initiate a \$250,000 wire to a bank account in Panama provided by CW-1 to facilitate a Bitcoin purchase. To proceed with the wire, MILLAN's bank requested additional documentation supporting the purpose of the wire. MILLAN asked CW-1 to provide her with a fake invoice for her to submit to her bank. CW-1's partner ("Individual-1") provided MILLAN with an invoice purporting to charge MILLAN \$250,000 for certain marketing services. MILLAN's bank left her a voicemail (which she sent to CW-1 and CW-1 provided to law enforcement) explaining the transaction could not be processed with the invoice she provided. Rather than proceed with the wire, MILLAN instead purchased a cashier's check payable to RODRIGUEZ in the amount of \$250,000.

c. After July 2018, MILLAN instead arranged to meet with CW-1 (or others working with CW-1) in person in the United States for the purpose of dropping off large sums of cash. At a February 2019 meeting, MILLAN provided CW-1 with \$400,000 cash in the parking lot of a hotel in Orlando, Florida. Following CW-1's arrest in mid-2019, MILLAN continued to deliver cash with CW-1 and sent CW-1 smaller wires; CW-1 sent MILLAN Bitcoin from an

---

obtaining a cooperation agreement and leniency at sentencing. CW-1's information has proved to be reliable and has been corroborated by other evidence.

undercover Coinbase account controlled by HSI. According to records maintained by HSI and CW-1, CW-1 sold MILLAN \$1.6 million in Bitcoin from 2018 to the present.

15. Based on my review of bank records, cryptocurrency transactions, and information obtained pursuant to email and cellphone search warrants, I have learned that in or around May 2019, HUGHES sold \$893,000 worth of Bitcoin from RODRIGUEZ to fund the purchase of the SUBJECT PREMISES for MILLAN. Based on my involvement in the investigation and my review of the financial transactions involved in the purchase of the SUBJECT PREMISES, I believe that the SUBJECT PREMISES was purchased with Victim money.

**There is Probable Cause to Believe that Records Relating to MILLAN's Involvement in the Airbit Club Scheme Will be Found at the SUBJECT PREMISES**

16. Based on my review of bank records and property records, I have learned that MILLAN purchased the SUBJECT PREMISES on or about May 21, 2019, and recorded the deed to the SUBJECT PREMISES in Guilford County, North Carolina, on or about May 22, 2020. Prior to purchasing the SUBJECT PREMISES, MILLAN owned and resided in a home in Raleigh, North Carolina (the "Raleigh Address"). Bank account records and cellphone records associated with MILLAN still list the Raleigh Address.

17. Based on my involvement in the investigation and my conversations with other law enforcement agents, I know that between in or around March 2020 and in or around May 2020, law enforcement agents drove by the SUBJECT PREMISES approximately two or three times each week and observed a vehicle registered to MILLAN parked in the driveway on multiple occasions. On or about July 30, 2020, law enforcement agents conducting surveillance identified MILLAN standing outside the SUBJECT PREMISES. Law enforcement agents conducting surveillance at the Raleigh Address in or around July and August 2020 have not seen MILLAN at the Raleigh Address.

18. Based on my review of MILLAN's travel records and information obtained pursuant to email, social media, and cellphone search warrants, I know that MILLAN traveled outside the United States multiple times each year from approximately 2016 until in or around January 2020 to promote the Airbit Club Scheme. Since in or around January 2020, MILLAN has not traveled internationally at all, presumably as a result of the global COVID-19 pandemic. Based on my conversations with Victim-1 and my review of a video of an Airbit Club promotional event on or about May 28, 2020, on the video conferencing platform Zoom that was consensually recorded by law enforcement agents at the invitation of Victim-1 (the "Zoom Conference"), I have learned that MILLAN is promoting Airbit Club from what appears to be a home office. Based on my review of a listing for the SUBJECT PREMISES on realtor.com (the "Realtor.com Listing"), including photographs of the interior of the SUBJECT PREMISES, I know that the SUBJECT PREMISES contains a home office. A photograph of the home office posted on the Realtor.com Listing shows a white built-in bookcase on the left side of the photograph that is set back slightly on a gray-green wall that is approximately six feet in length and abutted by another gray-green wall at a right angle. Based on my review of the recording of the Zoom Conference and my comparison to photographs from the Realtor.com Listing, MILLAN appears to be participating in the Zoom Conference from the home office inside the SUBJECT PREMISES. Based on my review of videos posted to MILLAN's public YouTube channel "Elite Team con Cecilia Millan" ("Elite Team with Cecilia Millan") and my review of the photographs posted on the Realtor.com Listing, I know that on or about April 16, 2020, and on or about June 10, 2020, MILLAN posted videos that appear to have been filmed inside the SUBJECT PREMISES. Based on the foregoing, there is probable cause to believe that MILLAN resides in the SUBJECT PREMISES.

19. Based on my training and experience, people typically maintain records related to their home purchase in their home, including escrow documentation, sales contracts, financial records, and deeds. As a result, there is probable cause to believe that records related to MILLAN's purchase of the SUBJECT PREMISES using the proceeds of the Airbit Club Scheme will be found in the SUBJECT PREMISES; that is, her purchase of the SUBJECT PREMISES using the proceeds of the Subject Offenses.

20. Based on my training and experience, it is likely that electronic devices containing digital records associated with the previously mentioned financial records, email correspondence, and online database records are maintained at the SUBJECT PREMISES. There is probable cause to believe that individuals such as MILLAN, who have a substantial online presence and regularly visit internet-based databases, websites, and email services, and post to public social media profiles, use a variety of electronic devices, such as laptop computers, desktop computers, tablets, smart phones, and other digital media means, to access the internet. Furthermore, based on my training and experience, there is probable cause to believe that MILLAN uses electronic devices to store electronic data related to the scheme.

21. Information obtained pursuant to email, social media, and cellphone search warrants, public social media posts, and the Zoom Conference described above demonstrate that MILLAN is utilizing a laptop, smart phone, or other mobile device to further the Airbit Club Scheme. For example, based on my training and experience, I know that MILLAN must have used either a laptop or a smartphone or other mobile device to host the Zoom Conference. Additionally, on or about April 16, 2020, on or about May 22, 2020, and on or about July 7, 2020, MILLAN posted promotional materials bearing MILLAN's photograph and the Airbit Club logo on her public Instagram account, "cecilia.millan\_eliteteam". Based on my training and experience,

MILLAN must have used a smartphone or other mobile device to post these promotional materials on Instagram.

22. Based upon my training, experience, and participation in investigations involving violations of financial crimes and related offenses, and my discussions with investigators involved in similar investigations, I know that businesses typically store their business records at the location from which they are working. Such records would include bank statements, check stubs, checks, deposit slips, payment records, invoices, correspondence with customers and others, emails, faxes, letterheads, and client files. These records can be maintained in paper form or electronically filed on laptops, smartphones, and other digital storage devices.

23. As described above, MILLAN has engaged in Bitcoin transactions in order to launder the proceeds of the Airbit Club Scheme. Based on my training and experience, I know that exchangers and users of cryptocurrencies store and transact their cryptocurrency in accounts commonly referred to as “wallets,” which are essentially digital accounts. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track transactions. A cryptocurrency user can store and access wallet software in a variety of forms, including via:

- a PC or laptop (“desktop wallet”),
- a mobile application on a smartphone or tablet (“mobile wallet”),
- an Internet-based cloud storage provider (“online wallet”),
- an online account associated with a cryptocurrency exchange (“online account”),
- a tangible, external device, such as a USB thumb drive (“hardware wallet”), or
- printed public and private keys (“paper wallet”).

Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other



commercially available device designed to store cryptocurrency (e.g., Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code<sup>5</sup> with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up via, for example, paper printouts, USB drives, or CDs. Wallets can be accessed through a password or a “recovery seed,” that is, random words strung together in a phrase. Based on my training and experience, I know that individuals who use cryptocurrency store their cryptocurrency wallets on their mobile devices, laptops, or on hard copy media in their homes. Therefore, there is probable cause to believe that evidence of MILLAN’s cryptocurrency transactions in furtherance of the Airbit Club Scheme will be found in the SUBJECT PREMISES.

#### **Computers, Electronic Storage, and Forensic Analysis**

24. As described in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, identified in Attachment A in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe records will be stored on that computer or storage medium, for at least the following reasons:

---

<sup>5</sup> A QR code is a matrix barcode that is a machine-readable optical label.

- a. Based on my training and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file — for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have

been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

26. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium, but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and “chat” programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. (A storage medium is any physical object upon which computer data can be recorded.

Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.) This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. Registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

27. In most cases, a thorough search of the premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy known as a mirror image of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the



volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

29. It is possible that the SUBJECT PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found

on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

### **CONCLUSION**

30. Based upon my training and experience and the investigation described above, I submit that there is probable cause to believe that MILLAN has violated the criminal statutes listed above and that evidence, fruits, and instrumentalities of these crimes as described in Attachment B are contained within the SUBJECT PREMISES, described in Attachment A.

on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.


**CONCLUSION**

30. Based upon my training and experience and the investigation described above, I submit that there is probable cause to believe that MILLAN has violated the criminal statutes listed above and that evidence, fruits, and instrumentalities of these crimes as described in Attachment B are contained within the SUBJECT PREMISES, described in Attachment A.

Respectfully submitted,

/s/ Charles Parker  
CHARLES PARKER  
Special Agent  
Homeland Security Investigations

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 14<sup>th</sup> day of August, 2020, at 3:33 a.m./p.m. (p.m.)

  
\_\_\_\_\_  
HON. L. PATRICK AULD  
United States Magistrate Judge  
Middle District of North Carolina